УДК 004.056.5

А.С. Минаев[*]

ИССЛЕДОВАНИЕ МЕТОДОВ И РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ С ФЛЭШ-НАКОПИТЕЛЕЙ

Защита данных от несанкционированного копирования (НСК) – это, прежде всего, защита авторских прав владельцев информации (литературных изданий, статей, произведений музыки и живописи, фотографий и т.д.). Отсутствие такой защиты приводит не только к потере прибыли, но и другим неприятным последствиям. К сожалению, в настоящее время попытки нарушения авторских прав на объекты интеллектуальной собственности – регулярное и повсеместное явление (особенно в Российской Федерации). Недостаток эффективности правовой защиты интересов создателей и владельцев информации приводит к необходимости создания аппаратно-программных комплексов (АПК) их защиты.

---

[*] Работа представлена в отборочном туре программы У.М.Н.И.К. 2012 г. в рамках Седьмой научной студенческой конференции «Проблемы техногенной безопасности и устойчивого развития» ассоциации «Объединенный университет им. В.И. Вернадского» и выполнена под руководством д-ра техн. наук, профессора ФГБОУ ВПО «ТГТУ» В.Е. Дидриха.

Организации, работающие не первый год в сфере информационных технологий, обязаны пользоваться многофункциональными сложными АПК, выполняющими широкий спектр задач по защите информации от НСК. И доходы таких компаний соотносятся с затратами на обеспечение защиты. А что делать, к примеру, художникам, фотографам, журналистам, писателям, композиторам, для защиты своих произведений от кражи? А если они, к тому же, владеют лишь азами «компьютерной грамоты», не говоря уже об опыте использования СЗД от НСК? Им одним известно, сколько затрачивается усилий, времени и материальных средств для создания «конечного продукта» интеллектуальной собственности, а быть может, и настоящего произведения искусства. Из-за отсутствия на рынке программного обеспечения (ПО), отвечающего их требованиям и материальным возможностям, их «выстраданные» произведения становятся источником легкой наживы злоумышленника. Отсюда и вытекает необходимость разработки ПО, ориентированного на специфического потребителя.

Целью работы является обеспечение защиты данных от НСК с материальных носителей информации с накопителей на флэш-памяти с интерфейсом USB.

Разрабатываемый программный продукт предназначен для защиты данных от НСК потенциальным злоумышленником (в качестве которого рассматривается не только стороннее лицо, но и сам пользователь, получивший разрешение владельца информации на ознакомление с ней).

В разработку ПО входит следующий перечень работ:

1) постановка проблемы;
2) описание предметной области;
3) программная реализация СЗД от НСК;
4) отладка программы;
5) документирование.

Во время достижения поставленной цели были решены следующие задачи:

1. Произведен анализ существующих методов и средств защиты данных от НСК с носителей типа USB-накопитель, в результате которого был обнаружен их недостаток, а именно недостаточная защита данных от НСК пользователем, которому они были предоставлены.

2. Разработана модель средства защиты данных, основанная на криптографической защите данных с привязкой к накопителю и расшифрованием файлов в оперативную память.

3. Разработано алгоритмическое обеспечение средства защиты, а также путем анализа вариантов на основе функции полезности был выбран оптимальный криптографический алгоритм.

4. Программно реализована разработанная модель средства защиты данных от НСК с носителей типа USB-накопитель для файлов формата .txt, .jpg, .png, .tiff, .bmp, .tga, .wav.

На основе результатов анализа недостатков существующих СЗД от НСК с носителей типа USB-накопитель была предложена система, лишенная этих недостатков. В ходе проектирования системы было разработано ее алгоритмическое обеспечение и выбран критографический алгоритм, используемый в программной реализации данного средства. В соответствие с разработанным алгоритмическим обеспечением была осуществлена программная реализация данного СЗД от НСК с носителей типа USB-накопитель.

В составе программного продукта можно выделить два основных приложения:

1) «администраторское» – модуль предварительной обработки информации – кодирует открытые данные текстовых, графических, аудио- и видеофайлов на выбранный накопитель;

2) «клиентское» – модуль работы с защищенными файлами – производит декодирование в область оперативной памяти рабочей станции и представляет вниманию пользователя данные в исходном виде при помощи включенных в состав приложения модулей чтения, имеющих ограниченный функционал.

Для защиты от посторонних лиц возможно использование криптографических методов защиты информации (КМЗИ), но при этом ключ шифрования должен вычисляться алгоритмически и не должен быть известен пользователю, дабы не дать ему возможности копировать и тиражировать доступную ему информацию. Расшифрованные файлы не сохраняются на носителе или жестком диске компьютера, а после завершения работы они удаляются.

На внешнем рынке имеются такие конкурентные АПК защиты от НСК как:

1. Transcend Elite, TDK Trans-IT, SanDisk Cruzer Enterprise, Elecom PASS, PinPad USB Stick – реализуют парольные методы защиты (за исключением Elecom PASS, который комбинирует парольную аутентификацию с привязкой к заданному ранее типу эксплуатируемых ЭВМ), что способствует защите от НСК посторонним лицом, но не обеспечивает защиты от НСК самим пользователем, что, безусловно, является существенным недостатком, как и свойственная этим комплексам необходимость наличия специализированного аппаратного обеспечения (АО) (защитить можно только USB-накопитель того же производителя, но не любой).

2. Dekart Private Disk, Flash Disk Crypto, True Crypt – реализуют КМЗИ (наибольшим преимуществом среди них обладает True Crypt, так как, во-первых, он распространяется бесплатно; во-вторых, деко-

дирование защищенных файлов осуществляется не на жесткий диск рабочей станции, а только в область ее оперативной памяти).

Но, несмотря на частные преимущества, True Crypt не осуществляет привязки кодированных файлов к конкретному USB-накопителю и не содержит в своем составе ограниченных по функционалу модулей чтения декодированной информации, а значит, и не защищает от НСК самим пользователем. Теоретически, злоумышленник может скопировать защищенные файлы и на другой носитель, а если он обладает еще и ключевым файлом, то у него появляется возможность копировать и тиражировать похищенные данные. В случае с разрабатываемым ПО так поступить не получится.

Несколько слов о контингенте потенциальных покупателей и об объемах платежеспособного рынка: анализ поисковых запросов по ключевым словам, относящимся к данному ПО, и к деятельности по защите от НСК в целом, показал, что за последние 12 месяцев пользователи поисковой системы Яндекс обращались к ней со следующими запросами (приведены количества запросов в среднем за месяц):

1) защита авторских прав – 3141;
2) защита от копирования – 5869;
3) защиты персональных данных – 16 316;
4) криптографическая защита информации – 1724;
5) защита usb flash – 805.

Полученные результаты дают основания полагать, что рынок содержит множество потенциальных пользователей проектируемого ПО. Что касается схем распространения продукта, планируется осуществлять продажу сразу тремя возможными путями:

1) предоставлять функциональные возможности ПО в качестве услуги;
2) продажа лицензий (годовая подписка);
3) прямая продажа ПО.

Менее приоритетным из трех способов является прямая продажа, так как ПО защиты от НСК само вполне подвержено копированию, а это уже означает убытки. Так что целесообразнее осуществлять прямую продажу по завышенным ценам.

Цены конкурентных продуктов, реализующих парольную защиту, зависят в основном от цены требуемого накопителя того же производителя и составляют суммы в диапазоне от $15 до $25, хотя встречаются и более дорогие образцы – $217. Цены продуктов, реализующих КМЗИ, находятся в диапазоне от $19.95 до $65 (указаны суммы для случая прямой продажи ПО потребителю). Предусмотрены бесплатные периоды для ознакомления с продуктом, что является сейчас по-

пулярным направлением стимулирования продаж. С учетом ценовой политики конкурентов цена продукта при прямой продаже не должна превышать $5.

СПИСОК ЛИТЕРАТУРЫ

1. Анин, Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – СПб. : БХВ-Петербург, 2000. – 384 с.

2. Баричев, С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М. : Горячая линия – Телеком, 2002. – 175 с.

3. Белкин, П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных / П.Ю. Белкин, О.О. Михальский, А.С. Першаков. – М. : Радио и связь, 1999. – 169 с.

Кафедра «Информационные системы и защита информации»
ФГБОУ ВПО «ТГТУ»